INFORMATION TECHNOLOGY GOVERNANCE AND THE AIR FORCE

GRADUATE RESEARCH PROJECT

Joseph M. Trechter, Major, USAF

AFIT/IC4/ENG/06-07

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/IC4/ENG/06-07

INFORMATION TECHNOLOGY GOVERNANCE
AND THE AIR FORCE

GRADUATE RESEARCH PROJECT

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of C4I Systems

Joseph M. Trechter, B.S.

Major, USAF

June 2006

AFIT/IC4/ENG/06-07

INFORMATION TECHNOLOGY GOVERNANCE
AND THE AIR FORCE

Joseph M. Trechter
Major, USAF

Approved:

_____/signed/_____   _____
Robert F. Mills (Chairman)   date

_____/signed/_____   _____
Alan R. Heminger (Member)   date

Abstract

Increased reliance on technology while budgets are tightening makes our investments in information technology (IT) all the more critical. How do we know whether our expenditures on IT are providing commensurate value to our mission to "fly and fight [and win] in Air, Space and Cyberspace"? This paper employs an assessment technique used in industry and applies the technique to the various echelons of command within the Air Force, namely the Headquarters, Major Command, and Operating Base levels to determine what IT governance structures exist within the Air Force. This case study on IT governance in the Air Force was conducted based on personal interviews with knowledgeable personnel at each echelon of command.

Acknowledgements

Table of Contents

Introduction

Military budgets are tightening. The Air Force is cutting 40,000 positions [11:8] to re-capitalize weapon systems. Efficiencies gained from ever more powerful technology are a primary tool for more effectively accomplishing our mission despite having fewer airmen. Increased reliance on technology while budgets are tightening makes our investments in information technology (IT) all the more critical. How do we know whether our expenditures on IT are providing commensurate value to our mission to "fly and fight [and win] in Air, Space and Cyberspace?"

This paper will begin with a review on the importance of aligning IT capabilities with business operations to ensure that the technology and technology-related processes we adopt truly provide value to our operational missions. With the importance of alignment in place, the paper will explore how Information Technology Governance provides the framework for implementing the alignment between IT and our mission. The paper will then document a specific case study of IT Governance within the Air Force based on an assessment methodology developed at Massachusetts Institute of Technology Sloan's Center for Informational Systems Research. The case study will apply the assessment at the Headquarters Air Force, Major Command, and Base levels of leadership and seek to identify strengths and weaknesses of IT Governance within this snapshot of the Air Force

Aligning IT and Mission

In the commercial sector, successful companies are keenly aware of the importance of aligning their IT Strategies and Infrastructure with their Business Strategies and Organization [1:265]. Businesses operate primarily under a profit motive. Make money or go out of business. Successful businesses do not regularly make significant investments in their IT posture without

1

considering the return expected on the investment [2:1]. If the latest technology widget will not

help their bottom-line by opening up new markets or making existing markets more profitable,

then the widget will not likely be purchased. Ensuring that a business's IT initiatives support the

overall business functions of the company is called IT-Business Alignment [1:267]. While

strong IT alignment and governance structures do not necessarily cause mission success, they do

correlate quite well to successful operations [3:26].

As with most things, a picture is very helpful in understanding concepts like alignment

between IT capabilities and business operations. Several models have been developed and most

consist of four primary activities to keep in alignment: business strategy, IT strategy, business

organization, and IT infrastructure. Two prevalent models are shown in figures 1 and 2 and the

basis for alignment discussions in this paper are guided primarily by the Venkatraman and
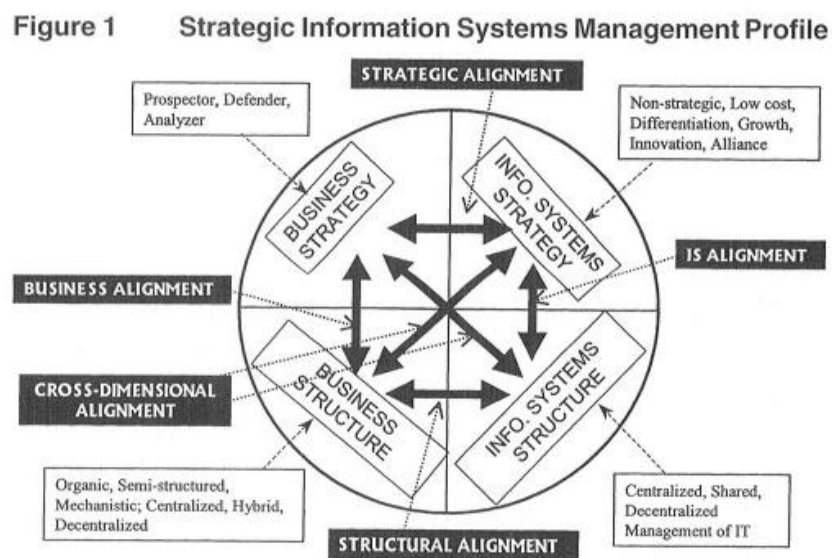
Henderson model in figure 2.

Figure 1. Strategic Information Systems Management Profile
By Sabherwal, Hirschheim, and Goles [6:314]
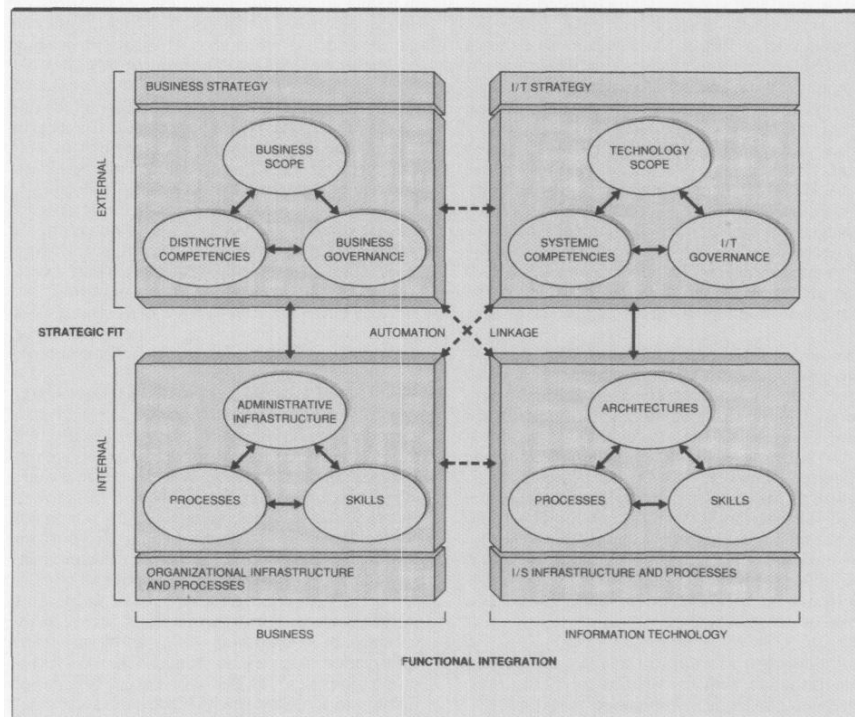
Figure 2: Strategic Alignment Model

Figure 2. Strategic Alignment Model
By Venkatraman and Henderson [4:476]

As is easily seen from the models, there are several axes of alignment. The focus of the

upper half of the model is strategy (either business or IT strategy), which primarily has an

external view – does our strategy empower us to compete with the greater marketplace? The

lower half of the model primarily has an internal focus based on the structures and processes that

drive day-to-day business [4:474]. The vertical alignment, then, reflects the degree to which an

organization creates its infrastructure and processes to support the defined strategy of the

organization. The horizontal alignment reflects the functional integration between the business

operations and the IT that supports those operations. Does the IT strategy flow from and support

the business strategy or does the IT strategy compete with or impede business strategy? Do the

organization's IT procedures and products help get the job done, or does the job get done despite

the IT infrastructure? There are also diagonal axes of alignment that reflect the level of

automation between the business strategy and the IT infrastructure as well as the linkage between organizational structure and the IT strategy.

Academic research has shown that when organizations fail to realize value from their investments in IT, the lack of alignment between business and IT strategies is often identified as a significant contributor [4:472]. Even when organizations invest the effort to align their business and IT practices, the effort must be ongoing and continuous to be successful [4:473]. Technology continues to advance rapidly and organizations continue to adapt to changing business opportunities, so the shared awareness between business and IT personnel that results from continuous alignment practices is crucial to maintaining operational advantages. In fact, a lack of alignment and a lack of shared awareness between the business and IT sides of an organization often degenerates to finger pointing rather than mutual trust if and when IT projects fail or become troubled [1:297].

While alignment between IT and business can certainly help avoid the pitfalls of wasted investments and finger pointing, strong alignment practices can also lead to revolutionary changes that take organizations to new and greater levels of performance. Periodic scrutiny of even well aligned organizations can challenge the status quo and move from simply tweaking structures and strategies to a higher level of identifying completely new ways of leveraging advancing technology together with new business perspectives to create or break into previously inaccessible realms of operation [6:341].

IT Governance

Alignment between business and IT activities is crucial to successful operations. How do organizations go about actually "doing" alignment? The broad-brush answer is IT Governance. "IT governance is the process by which firms align IT actions with their performance goals and

assign accountability for those actions and their outcomes [2:1]." During the process of governing, responsibility for making IT related decisions and accountability for the outcomes of the decisions must be explicitly assigned in order to encourage desirable use of IT assets [5:1], namely improving the organization's ability to conduct operations. Assigning responsibility and accountability may sound like elementary steps to take in articulating any process, but results of IT activities are typically difficult to measure [2:1] and therefore assigning responsibility for outcomes can also be difficult. Indeed, a significant barrier to effective IT governance is an overall lack of understanding about how decisions are made, what processes are to be implemented, and what behaviors are desirable [3:28]. If assigning responsibility and accountability were that simple, surely all organizations would have transparent accountability for governing IT decisions, but research has shown the opposite is more often true with an average of just one of three senior managers knowing how IT is governed in their own company [3:26].

Just as alignment must continuously be adjusted for changing conditions, the governing process must also be ongoing and deliberate to provide the framework necessary to harmonize each of the four activities within the alignment model [5:15]. Successful organizations not only make better IT decisions, they make successful decisions more consistently [5:1]. The best place for establishing governance for successful and consistent IT decisions is at the top. Senior leadership must be integral to the governing process and survey results indicate that senior management awareness of IT governance within the organization was the single best indicator for governance effectiveness [2:1]. This result makes sense since top level leadership is the ultimate source of assigning the responsibility and accountability so necessary to the governance process. "When senior managers take the time to design, implement, and communicate IT

governance processes, companies get more value from IT [3:26]" and realizing more value from IT is ultimately what we are interested in.

Assessing IT Governance

Hopefully the significance of business-IT alignment and IT governance for delivering more value from IT investments is beginning to sink in. With acceptance of the need for IT governance, a natural question becomes "how does my organization go about 'getting' IT governance?" From previous discussion, we know that senior leadership should be involved. We know there are four main areas to consider: business strategy, IT strategy, and business organization, and IT infrastructure. And we know whatever processes are developed should be on-going. These elements are all necessary, but there is no single recipe or model for IT governance that applies for all organizations. Some organizations will prefer a more centralized decision-making process, while others will prefer a more decentralized approach and still other will prefer a combination or hybrid between centralized and decentralized [3:29]. Since the organization is already making decisions (either by commission or omission) about IT investment, rather than asking how do we "get" IT governance, perhaps a better starting point is determining what type of IT governance is already taking place? A first step for any organization should be to evaluate their current governance structures (or lack thereof). Then an organization can determine its relative weaknesses and proceed to develop a more useful governance process based on the needs and goals of the organization.

Fortunately, researchers have been developing just such sets of assessment criteria and models for documenting an organization's IT governance structures. One of the foremost models is the "One Page" evaluation matrix developed by MIT Sloan's Center for Information Systems Research [2]. Their model is made up of two components: a numerical self-assessment

based on 4 factors and a matrix that documents how decisions are made within an organization about the implementation of IT in support of business operations. The focus of this case study will center on the decision matrix, but the results of the numerical self-assessments also offer insights on how organizations view their own structures for IT governance.

In the numerical self-assessment, organizations assigned an importance factor (i.e. importance of the outcome) as well as an influence factor (i.e. the influence of governance on the factor) for each of four possible outcomes of IT governance. Both importance and influence were rated on a scale of 1 to 5. The four possible outcomes of IT governance that were rated were:

- Cost Effective use of IT
- Effective Use of IT for growth
- Effective use of IT for asset utilization
- Effective use of IT for business flexibility

The numbers were then processed to produce a score from 0 to 100 reflecting the overall IT governance performance for the organization. This numerical self-assessment was completed for over 250 companies and while governance performance does vary significantly, the "take away" of the results is that performance is roughly bell-shaped [2:2]:

Average Governance Score	69
Minimum Score	20
Scored 80 or above	17%
Scored 90 or above	7%
Top Third of firms scored over 74	

These results are insightful and provide a view into how organizations are doing with regard to IT governance, but the set of possible outcomes does not map well to common measures of performance within the Air Force. For this reason, the numerical self-assessment

was not included in the case study interviews and is included here simply to highlight the general

performance of IT governance in industry.

Shifting focus to the decision making matrix aspect of MIT Sloan's governance

assessment model, the matrix documents who makes decisions about which aspects of IT

activities [2]. The columns of the matrix represent five domains where major decisions are made

with respect to management and use of IT in an organization. The rows of the matrix represent

the various decision-making levels or archetypes that make decisions. The template for the

matrix with the domains and archetypes are shown below in figure 3.

		Decision Domain				
		IT Principles	IT Architecture	IT Infrastructure	Business Applications	IT Investment
Governance Archetype	Business Monarchy					
	IT Monarchy					
	Federal					
	IT Duopoly					
	Feudal					
	Anarchy					

Figure 3

A few notes about the definitions of the domains and archetypes will be helpful to help
understand the distinctions of the matrix [2].

Archetypes

Business Monarchy	A senior business executive or a group of senior executives, sometimes including the CIO **[i.e. CSAF with or without the CIO]**
IT Monarchy	Individual or group of IT executives **[i.e. Air Staff]**
Federal	C-level executives (i.e. CEO, CIO, CFO) and business representatives of all the operating groups – may include IT involvement (equivalent of the central government and the states working together) **[i.e. Air Staff and all MAJCOMs]**
IT Duopoly	Two party decision making involving IT executives and one group of

8

	business leaders **[i.e. Air Staff and one MAJCOM]**
Feudal	Business unit or process leaders making separate decisions based on the needs of their entities **[i.e. MAJCOM HQ]**
Anarchy	Each individual or small group **[i.e. Comm Squadrons]**

Decision Domains

IT Principles	High-level decisions about the strategic role of IT in the business
IT Architecture	An integrated set of technical choices to guide the organization in satisfying business needs
IT Infrastructure Strategies	Centrally coordinated, shared IT services providing the foundation for the enterprise's IT capability and typically created before precise usage needs are known
Business Application Needs	Business requirements for purchased or internally developed IT applications
IT Investment	Decisions about how much and where to invest in IT, including project approval and justification techniques

As mentioned previously, there is no single recipe for effectively governing IT, so there may be any number of ways for successful organizations to complete the matrix. Research results have shown that organizations that emphasize efficient and standardized operations tend to implement a more centralized approach to decision making to maximize economies of scale. Organizations more focused on innovation and growth tend to implement more decentralized governing mechanisms so as to avoid limiting creativity [2:9]. Some organizations migrate from one method to another. Innovation is crucial to most "start-up" organizations, so a decentralized approach may be appropriate to impose as few oversight rules as possible in order to spur innovation and business growth. But as the organization grows over time, a more centralized approach may become necessary to take advantage of standardization and reuse efficiencies [2:10]. Still other organizations seek to balance standardization and innovation by implementing hybrid governing mechanisms somewhere in between centralized and decentralized [2:10]. Large global companies practically require a hybrid approach to governing to achieve the efficiencies of standardization while allowing sufficient autonomy to spur innovation. Many such companies implement tiered governance across several levels of the organization from the

enterprise level to a regional/group level to a business unit level [3:32]. This trend of hybrid governance that distributes accountability across multiple levels of large organizations will be especially applicable to this case study on governance within the Air Force, which can certainly be viewed as a large, global "company." Research indicates that some type of hybrid approach is quite common, but hybrid approaches also demand significant attention from management to keep the process working and flowing efficiently [2:10].

Methodology for Air Force Case Study

The primary purpose of this paper is to document a case study within the Air Force using the One Page decision making matrix to see how IT governance is implemented within at least a portion the Air Force enterprise. The case study considers three levels of leadership starting with the Headquarters of the Air Force (Air Staff) then to the Major Command (MAJCOM) and to the air force base level. Knowledgeable personnel were identified at each level to assist in completing the decision making matrix from their organization's perspective. Interviews were conducted after initial background information explaining the research and the decision making matrix was forwarded to each organization. Interviews were conducted in person or by phone and follow-up questions were carried out either via email or phone interaction. The ultimate goal of the interviews was to identify at what level within the organization decisions in each domain were made and also identify the specific actors or groups accountable for making the decisions.

For the headquarters level, many different offices play a role in governing the various domains. All of the interviewees at the headquarters level were from the staff of the Chief of Warfighting Integration and Chief Information Officer for the Office of the Secretary of the Air Force (SAF/XC) and for simplicity the group of people interviewed will be referred to as the "Air Staff." For the MAJCOM level, interviews were conducted with representatives from the

Air Force Materiel Command (AFMC) Communications Division (A-6) responsible for IT

governance within their command composed of bases and research centers through the United

States. At the base level of operations, insights were gathered with the Plans Division of the 88th

Communications Group from Wright Patterson AFB, Ohio. This case study was designed to

provide a snapshot of IT governance from different levels of leadership within the same chain of

command and ideally shed light on the level of integration between the different levels of

leadership with respect to IT decision making. Results from each level are detailed below

followed by a summation of the findings as they relate to IT governance as a whole.

Results of Case Study

Air Staff – SAF/XC

		Decision Domain				
		IT Principles	IT Architecture	IT Infrastructure	Business Applications	IT Investment
Governance Archetype	Business Monarchy	Sec of AF & CSAF SAF/XC: WIP				CSAF PPBE & AF Corporate Structure
	IT Monarchy		SAF/XC: AF EA	ESC PO: CITS	SAF/XC: SDC	
	Federal					
	IT Duopoly					
	Feudal					
	Anarchy					

Gathering interviews with the Air Staff was an ongoing effort that led me to at least seven

different offices that each had insights into IT governance within the Air Force. I suspect there

are other offices with useful insights as well that I didn't get the chance to talk with. Without

even asking a question, simply the number of people and offices involved in some way with IT

governance is a good indicator of the enormity of the task of governing IT within an enterprise of

hundreds of thousands of personnel spread across the entire globe carrying out a dizzying array of missions. Even with the wide array of "players" involved with IT governance, several observations can be distilled about IT governance as a whole.

On the topic of IT principles, there was wide agreement that the high-level role of IT within the AF was ultimately set by the Secretary of the AF and the Chief of Staff of the Air Force (CSAF). The CSAF Strategic Plan set out three primary goals for the Air Force: Win the Global War on Terror, Develop and Care for Airmen, and Recapitalize the Force. Ultimately, the role of IT is to support these goals. With the top level goals set by the CSAF, one could expect a more specific vision articulating how IT should support the top level goals. Not every office could put their finger on such a specific IT vision, but the primary office responsible for strategy and plans (SAF/XCXX – Strategy and Plans Division) did hold up the newly created Warfighting Integration Plan (WIP) as the current vision of IT within the Air Force. The WIP is a 77 page document just published in April 2006 that replaces the previously published C4ISR Roadmap. The WIP uses the goals of the CSAF Strategic Plan and identifies three domains to focus IT efforts toward those goals: warfighting (labeled C2ISR in the document), operational support, and infrastructure (labeled AF NetOps in the document) and each domain lists several goals for IT. One such goal from the C2ISR domain is to provide "Predictive Battlespace Awareness," which is further clarified to mean providing capability to allow commanders to predict and preempt enemy courses of action. Each domain has several such goals and together the goals address the entire spectrum of IT service areas from training and personnel to infrastructure to operational command and control. As a document, the WIP can be a useful source of guidance in identifying and carrying out IT projects, but the document is new and the real measure of the WIP's usefulness will be in how the document is used in practice over time

to guide IT investments. If the WIP becomes integral to prioritizing which IT services to pursue and fund, then it could fulfill the role of articulating the IT principles necessary for effective governance. But if the WIP is just another document that sounds good and fulfills a compliance requirement for higher level directives without really being used in practice, then the vision necessary for good IT governance will remain undefined.

In the architecture domain, the Architecture and Standards Division (SAF/XCXA) has several branches committed to developing and maintaining architectures and the policy that guides them. Several interviewees referenced the Air Force Enterprise Architecture Framework as the governing document for this domain, but the real architectural details are not in the Framework, but rather in the AF Enterprise Architecture (AF EA) itself which is captured in a "living" model using the Troux Metis application. In order to keep things manageable, the Air Force Enterprise Architecture has been sub-divided into three sub-architectures that correspond directly to the three domains outlined in the WIP: C2 Constellation Architecture (warfighting), Operational Support, and ConstellationNet (infrastructure). Each of these sub-architectures is encompassed in the Metis model which gives the ability to "drill down" from the top level enterprise all the way down to authoritative data sources such as AF Enterprise IT Data Repository (EITDR) and AF Infostructure Technical Reference Model (iTRM). While the model is not completely populated, it does provide a framework for documenting the core processes of the AF enterprise and the data integral to each process. The links between the AF EA and the lower level data sources like EITDR and iTRM are especially significant because these lower level data sources are the ones actively being used at MAJCOM level and below (when the lower levels are actually tracking the data). As with the WIP, the AF EA is potentially a very useful instrument for governing IT, but the real utility depends on its use in practice.

There is currently no direct link between funding and the EA. If an IT project diverges from the architecture, there is no mechanism short of a general officer steering group (3-star level) to affect funding and enforce adherence to the architecture. Mechanisms to enforce the architecture at lower levels would be more effective in developing systems that use existing capability and would ideally lead to projects starting with the architecture at the beginning of a new project rather than developing a project and then doing the minimum required to "comply" with the architecture after-the-fact.

Discussions with interviewees about infrastructure decisions did not get particularly specific, but most discussions culminated with the CITS program (Combat Information Transport System) managed by the Electronic Systems Center (ESC). CITS is an ongoing, billion dollar program to improve IT infrastructure at all Air Force sponsored operating locations. The CITS program works to develop and implement plans to improve the infrastructure backbone to include physical media like fiber optic cabling as well as some hardware equipment like routers and switches at Air Force locations. From the inputs gathered, CITS was largely characterized as something "out there" that more or less autonomously goes about prioritizing and providing service for AF bases around the globe. The CITS program office is accountable to higher ups and surely gets direction in how they prioritize their efforts, but insights into that prioritization process did not emerge from the interviews. Since the details of how CITS does its job is beyond the scope of this case study, no further efforts were devoted to documenting how CITS executes its program. The bottom line in terms of the decision making matrix is that a group made up of IT executives makes the decisions somewhere above the MAJCOM level.

As with the infrastructure domain, discussion about the business application domain did not get particularly specific, but most dialogue came back to the recently released Standard Desktop Configuration (SDC) policy released by SAF/XC mandating a standardized desktop of services. While the SDC business applications provide the minimum suite of applications that should be available throughout the AF enterprise, specialized applications can still be added to the SDC to accomplish mission objectives. Major Commands and units beneath the MAJCOM retain the authority to add approved applications to their systems depending on the requirements of the mission.

Of all the decision domains, IT Investment was certainly the area that drew the most pointed responses, for better or worse. Basically, IT investments are treated no differently than any other investment in the Air Force. The Planning, Programming, Budgeting, and Execution (PPBE) process applies to IT the same way it does to acquiring airplanes and other weapon systems. Each office interviewed quickly agreed that funding for IT was ultimately determined by the CSAF through the Program Objective Memorandum (POM) cycle process executed in PPBE. The Air Force Corporate Structure uses a series of panels, groups, boards, and councils to consolidate and prepare the overall POM submission for the CSAF. At lowest level of the Corporate Structure are panels that represent just about every functional area of the Air Force. There is Communications and Information Panel that coordinates and filters requests for IT projects. For an IT initiative to ultimately be accepted into the POM, it must be approved by the appropriate panel before it can be considered in sequence at higher levels of authority through the AF Group (roughly O-6 level), AF Board (roughly O-7/8 level), and AF Council (roughly O-9 level). This well established funding process has its strengths and weaknesses and will be

discussed further in the Summary of Findings section. For now, the salient point is that from the

Air Staff perspective, the IT investment decisions are made by a Business Monarchy.

MAJCOM - AFMC/A6

		Decision Domain				
		IT Principles	IT Architecture	IT Infrastructure	Business Applications	IT Investment
Governance Archetype	Business Monarchy	Congress: CCA CSAF: AF Strategy SAF/XC				CSAF and POM cycle (PPBE)
	IT Monarchy		SAF/XC	SAF/XC and CITS	CCIR process NDAA approval	
	Federal					
	IT Duopoly			Inputs from MAJCOMs	MAJCOM A-6	
	Feudal					
	Anarchy					

From the MAJCOM perspective at Air Force Materiel Command (AFMC), most of the

governance leadership resides at the Air Staff level, though the MAJCOM often has the

opportunity for inputs on plans and strategies as they are being developed. While noting that IT

principles within the Air Force are set in accordance with direction from the CSAF, the comment

was also made that Congress ultimately helped shape the role of IT by dictating certain desired

behaviors and investment tracking practices in the Clinger Cohen Act in 1996.

In the domain of IT architectures, there was no hesitation in identifying the architectures

division at Air Staff (i.e. IT monarchy) as the primary decision maker when it came down to

guiding architecture development and enforcement. But that doesn't mean the MAJCOM has no

role with the IT architecture as the MAJCOM has the opportunity to provide inputs and feedback

to architecture documents developed at Air Staff as well as the opportunity to develop

architectures reflective of the business practices within their MAJCOM. AFMC was a pioneer in

using the Enterprise Information Technology Data Repository (EITDR) before the Air Force as a whole began to take advantage of the system. AFMC used EITDR to store data about the various business systems (i.e. supply and finance tracking) used throughout the command and in fact has been successful in identifying unnecessary data redundancies enabling the command to delete and/or consolidate over 100 applications and save millions of dollars over the past 12 months. While EITDR is continually being populated with more detailed data flows about each application, there is also synergy within the architecture landscape because as mentioned in the discussion about architecture at the Air Staff level, data from EITDR is included in the Metis model reflecting the AF level architecture, so architecture information is gathered once and integrated into the overall architecture without re-entering volumes of data.

Both the infrastructure and business application domains are reflective of IT Monarchy decision making with IT leadership at levels above MAJCOM, but decisions are often based on inputs received from the MAJCOMs. Discussion during the interview about infrastructure eventually traced back to the CITS program that was also mentioned by the Air Staff as the primary infrastructure decision-making entity. Within AFMC, solid progress has been made using EITDR to document the applications used for various process flows and similar efforts are under way to document existing infrastructure equipment. One of the factors helping to drive infrastructure documentation is the eventual adoption of Internet Protocol version 6 (IPv6). There is a requirement to know by 2008 what infrastructure used by your organization can support IPv6 and what infrastructure cannot. In the process of analyzing the infrastructure capabilities for IPv6 adoption, the infrastructure is also being more consistently documented to create a blueprint of what infrastructure is located where. Business application decisions have historically been under the purview of the major commands in a more feudal archetype of

decision making. MAJCOMs have made Capital Investment Reports (CIRs) at the Air Staff for

some time to report on the status of their application projects, but the real approval to begin new

initiatives rested primarily with each MAJCOM. In compliance with the National Defense

Acquisition Act (NDAA) within the last couple of years, new applications or new functionality

to existing applications must be approved at the Department of Defense level, so while

MAJCOMs continue to be involved in developing business applications, the actual decision

making capacity primarily resides with IT leaders above MAJCOM level.

In terms of IT investments, as with the Air Staff feedback, the PPBE process is the

primary forum for deciding what programs receive funding. MAJCOMs are responsible for

preparing POM inputs to forecast spending needs at least 24 months in advance. One of the

frustrations of the process from the MAJCOM perspective is that the money actually budgeted to

them is invariably linked to the budget "they got last year," which often looks much different

that the inputs actually submitted.

Base Level - 88th Communications Group (AFMC)

<table>
<tr><td colspan="2" rowspan="2"></td><td colspan="5" align="center">Decision Domain</td></tr>
<tr><td>IT Principles</td><td>IT Architecture</td><td>IT Infrastructure</td><td>Business Applications</td><td>IT Investment</td></tr>
<tr><td rowspan="6">Governance Archetype</td><td>Business Monarchy</td><td>CSAF: 1 AF, 1 Network</td><td></td><td></td><td></td><td></td></tr>
<tr><td>IT Monarchy</td><td></td><td>Someone at MAJCOM or higher does architecture; not sure who</td><td></td><td>SAF/XC directed SDC</td><td>SAF/XC and MAJCOM A-6 dictate what funding is available</td></tr>
<tr><td>Federal</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>IT Duopoly</td><td></td><td></td><td>CITS program works with bases; Implement what is downward directed</td><td></td><td></td></tr>
<tr><td>Feudal</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Anarchy</td><td></td><td></td><td></td><td>Centers within AFMC make their own decisions</td><td></td></tr>
</table>

As a whole, the perspectives from base level on decision making match the perspectives

from the MAJCOM level, though in some cases decisions are made "up there" and it's difficult

to distinguish from the base level whether the decision was made at the MAJCOM, Air Staff, or

CSAF level. And from a base level viewpoint, it doesn't necessarily matter where "up there" a

decision was made - the bottom line is the decision must be followed at base level regardless of

who above them made the decision. Examples of IT principles as they filtered to base level is the

One Air Force…One Network initiative that began in 2000 and the AF NetOps plans to

consolidate down to a couple of Network Operations and Security Centers. IT architecture is an

area where the base level is aware that architectures exist, but there is little need to know exactly

where they came from (i.e. MAJCOM vs. Air Staff). By the time priorities are set for base level

implementation, the applicable architectures should have been consulted already so the base

level can focus on implementation. IT infrastructure discussions during the interview identified

the CITS program and also highlighted the interaction between base level and the CITS

personnel to help create the best infrastructure plans possible to balance both the long-term

infrastructure viability and the shorter-term impacts to operational users. Business application

issues at the base level, especially with the release of the Standard Desktop Configuration, tend

to fall into two categories. First there is the Standard Desktop Configuration, which base level

communications units will be responsible for working and second there are specialty applications

run in various organizations and Centers. Within AFMC, areas of functional expertise are

organized into Centers like the Electronic Systems Center and the Aeronautical Systems Center.

Each Center has a deputy chief information officer (DCIO) responsible for implementing

business applications necessary for their Center. While base level organizations must support the

Centers for compliance with the standard desktop configuration, additional applications are the

concern of the DCIOs so base level is not often involved with sorting out such specialty

applications. Investment decisions from the base level perspective emanate from the MAJCOM.

Base level units usually end up with little "discretionary" spending flexibility. Base level is

given a budget and an associated list of priorities from the MAJCOM that they must execute with

the allocated budget. Often, there is less budget than priorities, so additional hardware, software

or training requirements must be specially requested for supplementary (i.e. "fallout") funding.

Summary of Findings

Overall, there is a high degree of agreement between the different levels of command

about where IT governance decisions are made. The top business level of the Air Force, namely

the Chief of Staff, ultimately sets the vision for IT and decides how to invest in IT. The

architecture, infrastructure and business application domains are primarily the responsibility of

the Air Staff, although MAJCOM and base level organizations make vital contributions on how

these domains should be effectively governed.

Elements of Effective Governance Exist. The interview process revealed a fair amount

of knowledge resident in the various offices about the importance of IT governance and making

decisions for the benefit of the enterprise as a whole. The Air Staff has several branches within

its divisions dedicated to the various domains of IT decision making whether it is setting the

vision or strategy, defining architectures, or shepherding the funding process. The Warfighting

Integration Plan has the potential to provide useful guidance throughout the enterprise to ensure

all of our IT projects are ultimately providing value to our operators. The Metis tool used in the

architecture community appears to have bright promise in pulling many disparate architectures

together and creating a living and useful model of the Air Force enterprise. The EITDR and

iTRM applications are used at the MAJCOM and base levels to document aspects of the data

encompassed in the architecture and both of these applications are included as authoritative sources in the Metis tool used by the Air Staff to document the AF Enterprise as a whole. While the WIP and Metis efforts indicate we are making progress as an enterprise in documenting things necessary for making governance decisions, the real measure of success will be how those tools are used over time. Will the offices controlling purse strings be bound to follow these documents or will the documents be maintained just for the sake of being maintained? Will programs planning to largely duplicate efforts or diverge from existing architectures be held accountable to change their plans?

Assigning Accountability is Crucial. Accountability for decision making is paramount for effective governing. If no one is designated to ensure visions and architectures are developed and then also given the authority to hold programs accountable to the vision and architecture, then governance will remain unattainable. The re-merging of information technology related staffs under one boss in SAF/XC could go a good ways toward creating a single office accountable for creating a meaningful vision and architecture for IT investments. Even with a solid vision and architecture, tight integration into the funding process is also crucial to effective governance.

Link Architecture and Funding. This link between architecture and funding is crucial to ensuring our IT practices provide value to the Air Force mission by only funding those projects that increase our operational capabilities based on alignment with the target enterprise architecture. The current panel structure at the foundation of the Corporate Structure and PPBE process does include a Communications and Information panel that largely reviews IT projects, but there is nothing precluding other panels such as Information Support or Logistics from advocating the development of competing or similar IT projects. In some respects the panels

compete with each other for "scarce" dollars and that competition should be settled based on which project better fulfills a need within the architecture rather than settled based on how much money was awarded last year. If there is no overarching architecture designed to fulfill the vision of how IT should best support the mission, then there is no template to which projects can be held accountable. We appear to be making progress toward a clear vision and architecture, but the hard work making these elements integral to the governing process remains a work in progress.

Communicate the Governing Process. An important aspect of developing an effective vision and architecture is communicating how these elements contribute to making IT decisions. Both the WIP and the architecture captured in Metis are new within the last year and several years respectively. For these efforts to bear fruit in governing IT decisions throughout the enterprise, their utility and importance must be communicated over and over again through the enterprise. How well these efforts are communicated will go a long way toward entrenching them into the fund cycle and decision making processes.

The more reliance is placed on information technology to deliver greater combat capabilities and the more information technology is expected to "fill the gap" of a smaller work force in the Air Force, then the more important effective IT governance becomes. "The alternative to governance is an uncoordinated set of mechanisms implemented at different times, each addressing a specific and often local issue [5:17]." Continually solving local issues without due consideration to the greater enterprise is expensive and inefficient. Effective governance requires responsibility and accountability for providing IT capabilities that provide value to the mission and this accountability must reside at the top of the organization structure. With the reconsolidation of SAF/XC, clear accountability may be within reach to take advantage of

several existing mechanisms and ultimately provide the governance necessary for fielding effective IT projects. Accountability must also include appropriate funding controls to provide the hammer for projects that stray from the accepted vision and architecture of the enterprise. The Air Force doesn't have the option of simply "shutting down" for 6-12 months to completely rework processes and IT capabilities, so incremental steps are necessary to evolve processes while the mission remains ongoing. There are positive steps being taken toward effective IT governance, but many more steps are required to get there.

Ideas for Future Research

This case study focused on the Air Staff, MAJCOM, and base levels, but lots of IT decisions are made and big budgets are executed through System Program Offices. Tracing IT governance through the SPO structure might shed more light on how systems could more effectively be acquired so they integrate better into operations from the beginning.

The goals and architectures developed at the Air Staff tend to include the wide spectrum of IT capabilities from war fighting to home base business operations. The processes in place at MAJCOM and below are typically concerned with business operations with little emphasis on warfighting operations. Should there be a difference in how IT supports home base business operations versus warfighting operations versus acquisition operations?

Funding decisions ultimately drive which projects get pursued. With a clean sheet of paper, how could funding processes be designed to facilitate stronger governing practices?

Bibliography

1. Benbasat, I. and B.H. Reich. "Measuring the Information Systems-Business Strategy Relationship," in *Strategic Information Management*. Ed. Robert Galliers and Dorothy Leidner. Burlington, MA: Butterworth-Heineman, 2003.
2. Weill, P. and J.W. Ross. *IT Governance on One Page*. Sloan School of Management: Center for Information Systems Research, 2004 (CISR Working Paper No. 349).
3. Weill, P. and Jeanne Ross, "A Matrixed Approach to Designing IT Governance," *MIT Sloan Management Review*, 46, 2: 25-35 (Winter 2005).
4. Henderson, J.C. and N. Venkatraman, "Strategic Alignment: Leveraging Information Technology for Transforming Organizations," *IBM Systems Journal*, 32, 2/3: 472-484 (1999).
5. Weill, P. and R. Woodham. *Don't Just Lead, Govern: Implementing Effective IT Governance*. Sloan School of Management: Center for Information Systems Research, 2002 (CISR Working Paper No. 326).
6. Sabherwal, R., R. Hirschheim, and T. Goles. "Information Systems-Business Strategy Alignment," in *Strategic Information Management*. Ed. Robert Galliers and Dorothy Leidner. Burlington, MA: Butterworth-Heineman, 2003.
7. Peterson, R., R. O'Callaghan, and P. Ribbers, "Information Technology Governance by Design: Investigating Hybrid Configurations and Integration Mechanisms."
8. Salle, Mathias. *IT Service Management and IT Governance: Review, Comparative Analysis and their Impact on Utility Computing*. HP Laboratories, June 2, 2004 (HPL-2004-98).
9. Luftman, J.N., P.R. Lewis, and S.H. Oldach, "Transforming the Enterprise: The Alignment of Business and Information Technology Strategies," *IBM Systems Journal*, 32, 1:198-221 (1993).
10. De Haes, Steven and Wim Van Grembergen. *IT Governance Structures, Processes and Relational Mechanisms: Achieving IT/Business Alignment in a Major Belgian Financial Group*. Proceedings of the 38th Hawaii International Conference on System Sciences (2005).
11. Colarusso, Laura M. and Rod Hafemeister. "Forced Cuts," *The Air Force Times*, 66, 23:8-9 (26 December, 2005)

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
13-06-2006	**Graduate Research Project**	May 2005-Jun 2006

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information Technology Governance and the Air Force	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Trechter, Joseph, Major, USAF	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)	8. PERFORMING ORGANIZATION REPORT NUMBER
Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) 2950 Hobson Way WPAFB OH 45433-7765	AFIT/IC4/ENG/06-07

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
N/A	
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Increased reliance on technology while budgets are tightening makes our investments in information technology (IT) all the more critical. How do we know whether our expenditures on IT are providing commensurate value to our mission to "fly and fight [and win] in Air, Space and Cyberspace"? This paper employs an assessment technique used in industry and applies the technique to the various echelons of command within the Air Force, namely the Headquarters, Major Command, and Operating Base levels to determine what IT governance structures exist within the Air Force. This case study on IT governance in the Air Force was conducted based on personal interviews with knowledgeable personnel at each echelon of command.

15. SUBJECT TERMS
IT Governance, Business and IT Alignment

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
REPORT U	**ABSTRACT** U	**c. THIS PAGE** U	UU	31	**Robert F. Mills, PhD (ENG)** **19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-3636 ext 4527; email: Robert.mills@afit.edu